Exhibit H

RIDGEVIEW MEDICAL CENTER AND CLINICS #3511

SUBJECT: ENTERPRISE INFORMATION SECURITY GOVERNANCE POLICY

ORIGINATING DEPT: Information Technology (IT) **DISTRIBUTION DEPTS:** All

ACCREDITATION/REGULATORY STANDARDS:

Original Date: 12/12 **Revision Dates:** **Reviewed Dates:**	**APPROVAL:** Administration: _____ Director: _____

PURPOSE:

Introduction

Information security is a holistic discipline, meaning that its application or lack thereof affects all facets of an organization or enterprise. The goal of the Ridgeview Medical Center Information Security Program is to protect the Confidentiality, Integrity, and Availability of the data employed within the organization while providing value to the way we fulfill our mission. Protection of the Confidentiality, Integrity, and Availability are basic principles of information security, and can be defined as:

- ***Confidentiality*** – Ensuring that information is accessible only to those entities that are authorized to have access, many times enforced by the classic "need-to-know" principle.
- ***Integrity*** – Protecting the accuracy and completeness of information and the methods that are used to process and manage it.
- ***Availability*** – Ensuring that information assets (information, systems, facilities, networks, and computers) are accessible and usable when needed by an authorized entity.

Ridgeview Medical Center has recognized that our sensitive information is a critical asset and as such our ability to manage, control, and protect this asset will have a direct and significant impact on our future success.

This document establishes the framework from which other information security policies may be developed to ensure that the enterprise can efficiently and effectively manage, control and protect its business information assets and those information assets entrusted to Ridgeview Medical Center by its stakeholders, patients, partners, and other third-parties.

The Ridgeview Medical Center Information Security Program is built around the information contained within this policy and its supporting policies.

Purpose

The purpose of the Ridgeview Medical Center Enterprise Information Security Governance Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to Ridgeview Medical Center, its patients, business partners, and stakeholders. The Ridgeview Medical Center Enterprise Information Security Governance Policy is a reflection of management's views of information security, and serves as a framework document from which information security standards, guidelines, and procedures can be developed.

Sensitive information must be protected from unauthorized disclosure, theft, loss, and destruction. The compromise or loss of sensitive information can have an adverse effect on our competitive position and growth, the ability to comply with laws and regulations, and the integrity and trust inherent in the Ridgeview Medical Center name.

POLICY:

Scope

The Ridgeview Medical Center Enterprise Information Security Governance Policy applies equally to any individual, entity or process that interacts with any Ridgeview Medical Center Information Resource in any

tangible manner. Portions of this policy are more restrictive in scope than others, but all persons should read the policy in its entirety.

Responsibilities

Executive Management:

- Provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of Ridgeview Medical Center, and on information systems used or operated by Ridgeview Medical Center or by a contractor of Ridgeview Medical Center or other organization on behalf of Ridgeview Medical Center;
- Ensure that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of the organization;
- Ensure that information security processes are integrated with strategic and operational planning processes to secure the organization's mission;
- Ensure that senior management within the organization are given the necessary authority to secure the operations and assets under their control within the scope of Ridgeview Medical Center information security program;
- Designate a Director of Management Information Services and delegate authority to that individual to ensure compliance with applicable information security requirements; and
- Ensure that the Director of Management Information Services, in coordination with the other senior Ridgeview Medical Center managers, reports annually to Executive Management on the effectiveness of the Ridgeview Medical Center information security program, including the progress of remedial actions.
- An external Audit is conducted on an annual basis per 45 CFR Section 164.308(a)(1)(ii)(A) of the HIPAA Security Rule.

Director of Management Information Services:

- Ensure compliance with applicable information security requirements.
- Ensure preparation and maintenance of plans and procedures to address continuity of operations for information systems that support the operations and assets of Ridgeview Medical Center.
- Ensure that Ridgeview Medical Center has trained personnel to support compliance with information security policies, processes, standards, and guidelines.
- Report annually, in coordination with the other Ridgeview Medical Center senior managers, to Executive Management on the effectiveness of the Ridgeview Medical Center information security program, including progress of remedial actions.
- Head an office with the mission and resources to assist in ensuring company compliance with information security requirements.
- Assess risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of Ridgeview Medical Center.
- Develop and maintain information security policies, procedures, and control techniques to address all applicable requirements throughout the life cycle of each Ridgeview Medical Center information system.
- Facilitate development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems.
- Ensure that company personnel, including contractors, receive appropriate information security awareness training.

- Train and oversee personnel with significant responsibilities for information security with respect to such responsibilities, but not limited to, NAC, Wireless, Networking, VPN, etc.
- Implement and maintain a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of Ridgeview Medical Center.
- Develop and implement procedures for testing and evaluating the effectiveness of the Ridgeview Medical Center information security program in accordance with stated objectives.
- Review and manage the information security policy waiver request process.

All Ridgeview Medical Center Employees, Contractors, and Other 3rd-Party Personnel:

- Understand all of the information security policies that make up the Ridgeview Medical Center Information Security Program.
- Use Ridgeview Medical Center information and other information-related resources in compliance with all Ridgeview Medical Center Information Security Policies.
- Seek guidance from the Director of Management Information Services on information security related matters that are not clear.
- Communicate with the Director of Management Information Services and/or members of the Ridgeview Medical Center Information Security Committee regularly by providing feedback.

WAIVERS:

A waiver from a policy provision may be sought, and subsequently granted due to certain unforeseeable, unusual and/or exceptional circumstances. Policy provision waiver request, approval, and documentation procedures must be drafted and approved as part of this policy.

WAIVER REQUEST AND APPROVAL PROCESS:

1. The entity desiring to waive a policy provision shall complete Section 1 of the Ridgeview Medical Center Information Security Policy Waiver Request Form and forward it to the Ridgeview Medical Center Director of Management Information Services for review.
2. If the Ridgeview Medical Center Director of Management Information Services determines that there will be no adverse impact to security then he/she may make the decision to grant the waiver without the Ridgeview Medical Center Information Security Committee's consideration.
3. The Ridgeview Medical Center Information Security Committee will review the submitted Waiver Request form and conduct a thorough analysis to determine if the unusual and/or exceptional circumstances will introduce additional risk, or adversely impact the overall security of Ridgeview Medical Center, customer, or business partner.
4. The Ridgeview Medical Center Information Security Committee will also complete an analysis to determine if approval of a waiver for the exceptional circumstances would adversely affect compliance with any legal or regulatory requirements.
5. If the Ridgeview Medical Center Information Security Committee concurs, no further action is necessary. However, if there is non-concurrence, the final decision to approve the waiver may rest with the Ridgeview Medical Center Compliance Committee. The requestor should not assume concurrence until officially notified.
6. The requestor of the waiver will be notified of its status (approved, disapproved) in a timely manner.
7. If the acceptance of a waiver has the potential to introduce direct, additional risk to another party (i.e. business partner), a designated representative of that party, (preferably an executive) must send their concurrence to the Ridgeview Medical Center Director of Management Information Services (via e-mail, FAX, or regular mail) that the risk is acceptable before a waiver will be granted.

8. A record of the action taken on all waiver activity will be maintained by the Ridgeview Medical Center Information Security Committee.
9. The current Waiver Request form cited above is available on the Ridgeview Medical Center intranet site (RidgeNet).
10. All waivers must be reviewed annually.

ENFORCEMENT:

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights and termination of contract(s).

DEFINITIONS:

Information Resource - Considered in the broadest sense to include computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, fax servers, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Services (IS) - The name of the department responsible for the enterprise management of computers, networking and data access controls.

Mobile Device - Computing devices that are intended to be easily moved and/or carried for the convenience of the user, and to enable computing tasks without respect to location. Mobile devices include but are not limited to laptop computers, tablets, personal digital assistants (PDA), Smartphones, BlackBerry devices, cellular phones, and PocketPCs.

VERSION HISTORY OF SOURCE DOCUMENT: Ridgeview Medical Center Information Security Policy Manual

Version Number	Date	Reason/Comments
V1.00	December, 2012	Document Origination
V2.00	May, 2014	Full Review with IT Steering Committee
V3.00	August, 2015	Reviewed with Security Committee
	6/16	Finalized, assigned policy number, on RidgeNet. Previous documentation not archived.